REMARKS

This application has been carefully reviewed in light of the Final Office Action dated March 31, 2006, the Decision On Appeal dated May 28, 2008, and the Decision On Request For Rehearing dated October 29, 2008. Claims 1 to 3 and 8 to 46 are pending in the application, with Claims 4 to 7 having been canceled without prejudice or disclaimer of subject matter and without conceding the correctness of the rejection applied against them. Claims 1 and 33 are the independent claims. Reconsideration and further examination are respectfully requested.

In the Final Office Action dated March 31, 2006, all claims were rejected under 35 U.S.C. § 103(a). Independent Claim 1 was rejected over U.S. Application Publication No. 2002/0080391 (Sugiura) in view of U.S. Patent No. 6,816,270 (Cooper). Independent Claim 33 was rejected over Sugiura and Cooper in view of U.S. Patent No. 6,611,863 (Banginwar). The remaining claims are all dependent, and were rejected as above, or further in view of one or more of the following: U.S. Patent No. 6,240,456 (Teng), U.S. Patent No. 6,757,280 (Wilson), U.S. Patent No. 6,157,950 (Krishnan), U.S. Patent No. 6,020,973 (Levine), and U.S. Patent No. 6,742,039 (Remer). In response, Claims 4 to 7 have been cancelled without prejudice or disclaimer of subject matter and without conceding the correctness of any rejection, and the subject matter of Claims 4 to 7 has been incorporated into the independent claims. Accordingly, this should be viewed as a traversal of the rejections.

In addition to the above-noted changes, independent Claims 1 and 33 have also been amended to even further emphasize the nature of the claimed rules. In particular, Claims 1 and 33 now specify that the inbound rules table is used to determine whether an

application module in the computing device is to respond to an incoming message addressed to a target device, on behalf of the target device.

In view of these changes, the applied art is not seen to disclose or suggest the features of independent Claims 1 and 33, and withdrawal of the rejections is respectfully requested as explained more fully below.

Independent Claim 1 generally concerns mimicking network devices. A computing device has first and second network interface cards. The first network interface card connects the computing device to an external network, and the second network interface card connects the computing device to a local network. An incoming message is received from a client network device residing on an external network. The incoming message is addressed to a network address of a target network device residing on a local network. It is determined if an application module residing in a computing device is configured to process a functionality requested by the incoming message. The incoming message is redirected to the application module in the case that the application module is configured to process the functionality requested by the message, and the incoming message is passed through the local network to the target network device in the case that the application module is not configured to process the functionality requested by the message.

According to one example embodiment of the invention, an inbound rules table is used to determine if the functionality is to be processed by an application module residing in the computing device. The inbound rules table contains a plurality of rules, each rule corresponding to one of a plurality of target network devices on the local network. A target descriptor entry corresponding to each discovered target network device

is created in a target descriptor table, and a rule corresponding to each target descriptor entry is created in the inbound rules table. In addition, the inbound rules table contains at least one rule indicating whether a functionality requested for a corresponding target network device to perform is to be processed by an application module residing in the computing device. The processing by the application module includes responding to the incoming message addressed to the target device on behalf of the target device.

By virtue of these features, it is ordinarily possible to quickly and efficiently determine whether an application module in the computing device should respond to a message addressed to a target device, on behalf of the target device. Moreover, the rules table can be easily modified to account for new or different operations to be performed by the computing device on behalf of the target device.

Referring specifically to claim language, independent Claim 1 is directed to a method for mimicking network devices, the method being performed in a computing device having first and second network interface cards, the first network interface card connecting the computing device to an external network and the second network interface card connecting the computing device to a local network. The method includes discovering each of a plurality of target network devices on the local network by listening to the local network for messages from the target network devices, and creating a target descriptor entry corresponding to each discovered target network device in a target descriptor table. The method also includes creating a rule corresponding to each target descriptor entry in an inbound rules table containing a plurality of rules, wherein each rule corresponds to one of the plurality of target network devices on the local network and at least one rule indicates whether a functionality requested for a corresponding target

network device to perform is to be processed by an application module residing in the computing device. In addition, the method includes receiving, via the first network interface card, an incoming message from a client network device residing on the external network, the incoming message being addressed to a network address of a target network device residing on the local network. The method also includes determining if an application module residing in the computing device is configured to process a functionality requested by the incoming message, wherein the inbound rules table is used to determine if the functionality is to be processed by an application module residing in the computing device. The processing by the application module includes responding to the incoming message addressed to the target device on behalf of the target device. Additionally, the method includes redirecting the incoming message to the application module in the case that the application module is configured to process the functionality, and passing the incoming message through the local network via the second network interface card to the target network device residing on the local network in the case that the application module is not configured to process the functionality.

The applied art is not seen to disclose or suggest the features of Claim 1, and in particular is not seen to disclose or suggest at least the features of (i) using an inbound rules table to determine if a functionality requested by a message addressed to a target device is to be processed by an application module residing in the computing device, wherein the processing by the application module includes responding to the incoming message addressed to the target device on behalf of the target device, (ii) containing, within the inbound rules table, a plurality of rules, each rule corresponding to one of a plurality of target network devices on the local network, (iii) creating a target descriptor entry

corresponding to each discovered target network device in a target descriptor table, and creating a rule corresponding to each target descriptor entry in the inbound rules table, and (iv) containing, within the inbound rules table, at least one rule which indicates whether a functionality requested for a corresponding target network device to perform is to be processed by an application module residing in the computing device.

The Office Action, in its rejection of now-canceled Claims 4 to 7, concedes that Sugiura and Cooper do not disclose the above-noted features. Nevertheless, the Office Action relies on Banginwar for these features.

As understood by Applicants, Banginwar is directed to a technique for assigning devices to device proxies. Each device proxy registers a filter with a device discovery, identifying characteristics of devices that the device proxy will communicate with. The device discovery identifies the devices in the network that match the filter, and notifies the device proxy of the matching devices. The device proxy then distributes policies from a policy server to the devices which match its filter. See Banginwar, Abstract.

Page 10, 11 and 12 of the Office Action assert that Banginwar (Column 1, line 60 to Column 2, line 12, Column 2, lines 18 to 26, Column 4, lines 10 to 45 and Column 5, lines 7 to 29) discloses using an inbound rules table to determine if a functionality is to be processed by an application module residing in the computing device, wherein the inbound rules table contains a plurality of rules, each corresponding to one of a plurality of target network devices on the local network, and creating a target descriptor entry corresponding to each discovered target network device in a target descriptor table and creating a rule corresponding to each target descriptor entry in the inbound rules table,

wherein the inbound rules table contains at least one rule which indicates whether a functionality requested for a corresponding target network device to perform is to be processed by an application module residing in the computing device.

In this regard, the cited portions of Banginwar refer to two separate concepts: (1) Banginwar's control policies, and (2) Banginwar's filters.

Banginwar's control policies are simply policies for controlling proxy-managed devices. For example, a control policy can include blocking all packets between the hours of 9 a.m. and 5 p.m. See Banginwar, Column 2, lines 18 to 26.

Banginwar's filters, on the other hand, are simply the set of characteristics used to match Banginwar's device proxies to a set of devices. More specifically, Banginwar's device proxy registers a filter containing the characteristics of devices it will manage, and the filter is used to match discovered devices to the device proxy. See Banginwar, Column 1, line 60 to Column 2, line 12, Column 4, lines 10 to 45 and Column 5, lines 7 to 29.

However, there is no indication that each of Banginwar's policies or filters respectively corresponds to a single device. In fact, Banginwar suggests otherwise, as the purpose of the device proxy is to manage several devices at once.

Moreover, Banginwar's policies and filters differ fundamentally from the nature of the rules claimed by Applicants. In particular, there is no suggestion that any of Banginwar's policies or filters are used to determine whether another device should process a functionality specifically requested of the managed device, much less whether another device should process a functionality requested by a message from a client device on an external network which is addressed to a network address of the managed device.

As indicated above, Applicants have amended the claims to even further emphasize this distinction, such that the claims now specify that the inbound rules table is used to determine whether an application module in the computing device is to respond to an incoming message addressed to a target device, on behalf of the target device.

In view of the above, it logically follows that Banginwar does not disclose or suggest the features of Claim 1, including (i) using an inbound rules table to determine if a functionality requested by a message addressed to a target device is to be processed by an application module residing in the computing device, wherein the processing by the application module includes responding to the incoming message addressed to the target device on behalf of the target device, (ii) containing, within the inbound rules table, a plurality of rules, each rule corresponding to one of a plurality of target network devices on the local network, (iii) creating a target descriptor entry corresponding to each discovered target network device in a target descriptor table, and creating a rule corresponding to each target descriptor entry in the inbound rules table, and (iv) containing, within the inbound rules table, at least one rule which indicates whether a functionality requested for a corresponding target network device to perform is to be processed by an application module residing in the computing device.

Teng, Wilson, Krishnan, Levine, and Remer have been reviewed and are not seen to remedy the above-noted deficiencies of Sugiura, Cooper and Banginwar.

Therefore, independent Claim 1 is believed to be in condition for allowance, and such action is respectfully requested.

Independent Claim 33 also contains the features of now-canceled Claims 4 to 7, as well as the amendment to specify that the inbound rules table is used to determine

whether an application module in the computing device is to respond to an incoming message addressed to a target device, on behalf of the target device. Accordingly, Claim 33 is believed to be allowable over the applied art for at least the same reasons as Claim 1.

The other claims in the application are each dependent from the independent claims and are believed to be allowable over the applied references for at least the same reasons. Because each dependent claim is deemed to define an additional aspect of the invention, however, the individual consideration of each on its own merits is respectfully requested.

No other matters being raised, it is believed that the entire application is fully in condition for allowance, and such action is courteously solicited.

Applicants' undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

/Michael J. Guzniczak/
Michael J. Guzniczak
Attorney for Applicants
Registration No.: 59,820

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3800
Facsimile: (212) 218-2200

FCHS_WS 2702145v1